AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph beginning at page 9, line 7, with the following rewritten paragraph.

-- In the RSA encryption method, from two prime numbers p and q and one of the public keys E (public exponent), using Equations (1) and (2), the other public key, i.e., the public key N (modulus) and a private key D (private exponent) will be obtained. --

Please replace the paragraph beginning at page 10, line 8, with the following rewritten paragraph.

-- Since the key length is 512 bits, firstly, the random number generator 3 generates two 256-bit random numbers. These two random numbers serve as seeds, i.e., initial values for finding two prime numbers. --

Please replace the paragraph beginning at page 12, line 13, with the following rewritten paragraph.

-- As has been described above, the random number generator 3 generates a complete random number having a long periodicity by extracting the least significant bit of pixel values of pixels. The encryption means 4 generates two prime numbers p and q from the two random numbers generated by the random number generator 3. As shown in fig. 5, the encryption means 4 generates an encryption key through a prime number generation process and a key generation process. --

Please replace the paragraph beginning at page 17, line 3, with the following rewritten paragraph.

-- It should be noted that in the aforementioned embodiment, an explanation has been given on a case of generating a random number ~~form~~ from the least significant bits of pixel values of a gray scale image. However, the fingerprint identification apparatus can also generate a random number according to pixel values of the respective pixels of a binary image, and can generate a random number according to pixel values of respective pixels of a binary image as follows. Here, it is assumed that the horizontal direction address is i and the vertical direction address is j, and an arbitrary pixel on the binary image is b (i, j). --